

12 MAG 1656

Approved: Rosemary Nidiry
Rosemary Nidiry
Assistant United States Attorney

Before: HONORABLE ANDREW J. PECK
United States Magistrate Judge
Southern District of New York

- - - - - X
UNITED STATES OF AMERICA :
 : SEALED COMPLAINT
 :
 - v. - : Violation of
 : 18 U.S.C. §§ 1029(a)(3),
 JARAND MOEN ROMTVEIT, : 1029(a)(5), 1028A
 a/k/a "zer0," :
 a/k/a "zer0iq," : COUNTY OF OFFENSE:
 : New York
 :
 Defendant. :
 :
 - - - - - X

SOUTHERN DISTRICT OF NEW YORK, ss.:

JOHN LEO, JR., being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation ("FBI") and charges as follows:

COUNT ONE
(Access Device Fraud)

1. From at least in or about September 2010, up to and including in or about May 2012, in the Southern District of New York and elsewhere, JARAND MOEN ROMTVEIT, a/k/a "zer0," a/k/a "zer0iq," the defendant, knowingly and with intent to defraud, and affecting interstate and foreign commerce, possessed fifteen and more devices which were counterfeit and unauthorized access devices, to wit, ROMTVEIT possessed more than fifteen credit card numbers that he obtained by hacking into computer systems.

(Title 18, United States Code, Sections 1029(a)(3) and 2.)

COUNT TWO
(Access Device Fraud)

2. From at least in or about February 2012, up to and including in or about May 2012, in the Southern District of New York and elsewhere, JARAND MOEN ROMTVEIT, a/k/a "zer0," a/k/a "zer0iq," the defendant, knowingly and with intent to defraud, and affecting interstate and foreign commerce, effected transactions, with one or more access devices issued to another person or persons, to receive payment and any other thing of value during a 1-year period the aggregate value of which was equal to or greater than \$1,000, to wit, ROMTVEIT sold stolen credit card account information in exchange for approximately \$1,100 and a laptop computer.

(Title 18, United States Code, Sections 1029(a)(5) and 2.)

COUNT THREE
(Aggravated Identity Theft)

3. From at least in or about September 2010, up to and including in or about May 2012, in the Southern District of New York and elsewhere, JARAND MOEN ROMTVEIT, a/k/a "zer0," a/k/a "zer0iq," the defendant, willfully and knowingly did transfer and possess, without lawful authority, a means of identification of another person, during and in relation to the felony violation charged in Counts One and Two of this Complaint, to wit, ROMTVEIT transferred and possessed, among other things, the name, address, and credit card account number of another person in connection with his participation in access device fraud as charged in Counts One and Two of this Complaint.

(Title 18, United States Code, Sections 1028A(a)(1),
1028A(b), and 2.)

The bases for my knowledge and for the foregoing charges are, in part, as follows:

4. I have been personally involved in the investigation of this matter. This affidavit is based upon my investigation, my conversations with other law enforcement agents, and my examination of reports and records. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of

others are reported herein, they are reported in substance and in part, except where otherwise indicated.

5. I have been a Special Agent with the FBI for approximately six years. For the past approximately five years, I have been assigned to a computer intrusion squad in the FBI's New York Field Office. I have received extensive training regarding computer technology, computer fraud, and white collar crimes, and have participated in dozens of investigations involving computer intrusions, including investigations that resulted in the execution of search warrants and/or arrests.

BACKGROUND

6. Based on my training and experience, I have learned the following:

a. Carding: "Carding" refers to various criminal activities associated with stealing personal identification information and financial information belonging to other individuals - including the account information associated with credit cards, bank cards, debit cards, or other access devices - and using that information to obtain money, goods, or services without the victims' authorization or consent. For example, a criminal might gain unauthorized access to (or "hack") a database maintained on a computer server and steal credit card numbers and other personal information stored in that database. The criminal can then use the stolen information to, among other things: (1) buy goods or services online; (2) manufacture counterfeit credit cards by encoding them with the stolen account information; (3) manufacture false identification documents (which can be used in turn to facilitate fraudulent purchases); or (4) sell the stolen information to others who intend to use it for criminal purposes. "Carding" refers to the foregoing criminal activity generally and encompasses a variety of federal offenses, including, but not limited to, identification document fraud, aggravated identity theft, access device fraud, computer hacking, wire fraud, and bank fraud.

b. Carding Forums: "Carding forums" are websites used by criminals engaged in carding ("carders") to facilitate their criminal activity. Carders use carding forums to, among other things: (1) exchange information related to carding, such as information concerning hacking methods or computer-security vulnerabilities that could be used to obtain personal identification information; and (2) buy and sell goods and services related to carding, for example, stolen credit card or

debit card account numbers, hardware for creating counterfeit credit cards or debit cards, or goods bought with compromised credit card and debit card accounts. Carding forums often permit users to post public messages (postings that can be viewed by all users of the site), sometimes referred to as "threads." For example, a user who has stolen credit card numbers may post a public "thread" offering to sell the numbers. Carding forums also often permit users to communicate one-to-one through so-called "private messages." Because carding forums are, in essence, marketplaces for illegal activities, access is typically restricted to avoid law enforcement surveillance. Typically, a prospective user seeking to join a carding forum can only do so if other, already established users "vouch" for the prospective user, or if the prospective user pays a sum of money to the operators of the carding forum. User accounts are typically identified by a username and access is restricted by password. Users of carding forums typically identify themselves on such forums using aliases or online nicknames ("nics").

7. Based on my participation in the investigation of this matter, I know the following:

a. In or about June 2010, the FBI established an undercover carding forum (the "UC Site"), enabling users to discuss various topics related to carding and to communicate offers to buy, sell, and exchange goods and services related to carding, among other things.

b. The FBI established the UC Site as an online meeting place where the FBI could locate cybercriminals, investigate and identify them, and disrupt their activities.¹ The UC Site was configured to allow the FBI to monitor and to record the discussion threads posted to the site, as well as private messages sent through the site between registered users. The UC Site also allowed the FBI to record the Internet protocol ("IP") addresses of users' computers when they accessed the site.²

c. Access to the UC Site was limited to registered members and required a username and password to gain entry.

¹ The registration process for the UC Site required users to agree to terms and conditions, including that their activities on the UC Site were subject to monitoring for any purpose.

² Every computer on the Internet is identified by a unique number called an Internet protocol ("IP") address, which is used to route information properly between computers.

Various membership requirements were imposed from time to time to restrict site membership to individuals with established knowledge of carding techniques or interest in criminal activity. For example, at times new users were prevented from joining the site unless they were recommended by two existing users who had registered with the site, or unless they paid a registration fee.

d. New users registering with the UC Site were required to provide a valid e-mail address as part of the registration process. An e-mail message was sent to that email address containing registration instructions. In order to complete the registration process, the new user was required to open the e-mail, click on a link in it, and then enter an activation code specified in the e-mail message. The e-mail addresses entered by registered members of the site were collected by the FBI.

e. In the course of the undercover operation, the FBI contacted multiple affected institutions and/or individuals to advise them of discovered breaches in order to enable them to take appropriate responsive and protective measures. Based on information obtained through the site, the FBI estimates that it helped financial institutions prevent many millions of dollars in losses from credit card fraud and other criminal activity, and has alerted specific individuals regarding breaches of their personal email or other accounts.

f. At all times relevant to this Complaint, the server for the UC Site, through which all public and private messages on the UC Site were transmitted, was located in New York, New York.

THE INVESTIGATION

8. As set forth in greater detail below, the investigation has revealed that JARAND MOEN ROMTVEIT, a/k/a "zer0," a/k/a "zer0iq," the defendant, used hacking tools to access various databases, including the on-line account databases of banks. He offered to provide stolen credit card information in communications on-line with an individual he believed to be a UC Site Administrator; in fact, the individual was me, posing as a UC Site Administrator. In the course of the investigation, ROMTVEIT sent to me information from over 40 credit card accounts.

9. Based on my involvement in monitoring the UC Site and

my review of files and logs maintained by the FBI concerning the UC Site, I know that, on or about September 12, 2010, a new user registered on the UC Site with the username "zer0iq" and using the email address zer0iq@hotmail.com. "zer0iq" also used the email address jarandmoen@live.no on the UC Site on or about April 14, 2011. On or about November 2, 2010, a user registered on the UC Site with the username "zer0" and using the email address Woods19852@hotmail.com. In or about April 2011, the user "zer0iq" advised me, in my undercover capacity as the site administrator of the UC Site, that he was also the individual with the username "zer0" and asked for the accounts belonging to "zer0" and "zer0iq" on the UC Site to be merged, which they were, under the username "zer0". After the two user IDs were merged in this manner, "zer0iq" ceased to be used on the UC Site. Accordingly, I believe that a single individual used both the "zer0iq" and "zer0" nicknames on the UC Site. As set forth in greater detail in ¶¶18-21 below, this individual has been identified to be JARAND MOEN ROMTVEIT, a/k/a "zer0," a/k/a "zer0iq," the defendant.

10. Beginning in or about December 2010, while using an undercover online identity, I have been in periodic communication with JARAND MOEN ROMTVEIT, a/k/a "zer0," a/k/a "zer0iq," the defendant, through MSN Messenger, after the defendant, using the nickname "zer0," contacted me through the UC Site where I was posing as the site administrator. ("MSN Messenger" is an instant-message system on the Internet allowing users to "chat" online, that is, to send text messages back-and-forth to one another in near real time. Users are identified by email addresses.) I have reviewed those private MSN Messenger "chats," which were electronically preserved.

11. In a private chat with me on or about December 15, 2010, JARAND MOEN ROMTVEIT, a/k/a "zer0," a/k/a "zer0iq," the defendant, using the nickname "zer0," discussed his attempts to access the internal databases of a major U.S. bank ("Bank-1") and offered to send me a computer application, "SpyEye," that would steal information from Bank-1. He then stated that he had "gotten like 40 CCs in 4 days."³ Based on my involvement in this investigation, I believe that in this communication, the defendant was claiming to have obtained through this hacking application 40 credit cards in four days from Bank-1 without authorization. Based on my training and experience, I know that

³ Quotations from emails and online postings are reproduced substantially as they appear in the original text; that is, errors in spelling and punctuation have not been corrected.

SpyEye is a type of malicious software that is used to steal information relating to on-line bank accounts.

12. In a private chat with me on or about June 17, 2011, JARAND MOEN ROMTVEIT, a/k/a "zer0," a/k/a "zer0iq," the defendant, using the nickname "zer0," said: "webinjects just worked" and then pasted information from what appeared to be a bank customer, including the individual's name; email address; password; and security questions and answers to access the customer's account. Based on my experience with this investigation, I know that "webinjects" refers to malware developed by hackers to inject unauthorized content into the web pages of websites, usually of banks, through which they can then steal confidential information, including customers' account information. I believe that in this communication ROMTVEIT stated that the "webinjects" he had been working on had been successful and he pasted a compromised customer's bank account information in order to demonstrate that he had successfully obtained unauthorized access to confidential bank customer information. Because the information that the defendant provided to me did not include information such as the name of the bank or the account number, it was not possible to verify whether this was actual compromised bank account information.

13. In a series of private chats with me between on or about February 8 and February 9, 2012, JARAND MOEN ROMTVEIT, a/k/a "zer0," a/k/a "zer0iq," the defendant, using the nickname "zer0," discussed his access to various stolen credit card databases, and demonstrated to me how he was able to get such access, as set forth below:

a. In a chat on or about February 8, 2012, ROMTVEIT said: "i haven't ran a botnet in 4 months." I know based on my training and experience that a "botnet" refers to a group of computers which have been compromised by malware which causes them to perform automated tasks on the Internet without the legitimate computer owner's knowledge. In the chat, I then asked: "what have u been doing then?" to which the defendant responded, ". . . nothing much, just carding and hacking mostly. . . . grabbed 3k CC's but without cvv2." I asked, "still using them?" and he responded: "yeah sometimes on amazon for games." Based on my training and experience and involvement in this investigation, I believe that in this chat, ROMTVEIT was relaying that he had stolen account data for 3,000 credit cards (although without a security code, which is often found on the back of credit cards, called a "cvv" or "card verification value" number), some of which he was using on Amazon to purchase

online games. Approximately 15 minutes later, in the same chat, ROMTVEIT posted account data for three credit cards, including the account numbers, expiration dates, and the CVV for all three, and the name and address of the account holder for one of the three. Based on information from representatives of Visa, FBI agents have confirmed that the information for these three cards corresponded to genuine, active accounts belonging to individuals other than JARAND MOEN ROMTVEIT, a/k/a "zer0," a/k/a "zer0iq," the defendant.⁴

b. In a chat on or about February 9, 2012, ROMTVEIT again discussed credit cards that he had "from 10-12 sites i hacked worldwide." He later said: "Ive used the cards alot on amazon but only works for orders at ~100\$ overstock keeps canceling all my orders. gifcards, etc you name it." Based on my experience with this investigation, I believe that in this chat, ROMTVEIT discussed the various ways in which he used credit card information he had stolen, including purchases through Amazon and Overstock.com. Later in that same chat, the defendant asked me: "are you from the US," and I responded that I was in New York.

c. In a later chat on or about February 9, 2012, ROMTVEIT offered to demonstrate for me a program he had developed which "auto exploits the sites from google and pulls the database down, and decrypts the database." Through a computer program on both of our computers, I was able to view the defendant's computer screen as he used this program, which could identify websites with "shopping carts" - that is, websites from which individuals could place in online "shopping carts" items to be purchased with credit cards. As he was using the tool, the defendant explained, in a contemporaneous chat, "it autoexploits puts them into files . . . with full db and pass . . . Done! Counted 33 card infoz (without cvv#) out of 36 entries! Saved to file . . ." Based on my experience with this investigation, as well as my training and experience, I believe that in this chat ROMTVEIT was describing how the program exploits websites and enables the user to copy the contents, including any databases and passwords associated with the sites, into files for later access. I watched in real time as, with this program, the defendant was able to identify certain such websites, go into their databases, and steal what appeared to be

⁴ The FBI has notified the relevant credit card companies regarding all the credit card information transmitted by the defendant discussed both in this paragraph and referenced throughout this Complaint.

account information for at least 33 credit cards and copy that information and store it in separate files, which he would be able to access later. (Based on my subsequent review of the stolen account information, I determined that it did not include any complete credit card numbers, and therefore did not give ROMTVEIT access to fully identifiable credit card accounts.)

d. As described above, I viewed remotely the defendant's computer screen as he demonstrated the program discussed above. As a result, I was able to see that he had multiple windows open on his computer screen, and, on one of these I could see the name "Jarand Moen". Upon ending his demonstration of the program, the defendant said in the chat: "Well that's it tho, you got a small snippit . . . + my real name if you looked close lol [laugh out loud]." Based on my involvement in this investigation, I believe that ROMTVEIT was referring to the fact that his real name appeared on his computer screen and a viewer who looked closely would be able to learn his identity. Later in that same chat, the defendant provided me with the link to his Facebook account, www.facebook.com/jarandmr.

14. In a series of private chats between on or about February 24, 2012, and March 1, 2012, JARAND MOEN ROMTVEIT, a/k/a "zer0," a/k/a "zer0iq," the defendant, using the nickname "zer0," and I discussed a transaction in which ROMTVEIT would provide me with stolen credit card information in exchange for a laptop computer, as set forth below:

a. In a chat on or about February 24, 2012, ROMTVEIT wrote: "I got a few USA dumps, do you know anyone that can use them and maybe buy me something i'n return . . . Got 40 amex centurion 50 visa and 50 master." Based on my training and experience investigating carding crimes, I know that "dumps" is a term used by carders to refer to credit card data in the form in which such data is stored on the magnetic strips on the backs of credit cards. I believe that in this chat, the defendant offered to sell the stolen credit card data from 40 American Express "Centurion" cards, and 50 Visa and 50 Mastercards. In response, I asked "what u looking to get?"; ROMTVEIT eventually decided on an Apple laptop computer.

b. I agreed to send him the computer (the "Apple Laptop") in exchange for stolen credit card information. Subsequently, ROMTVEIT provided me with a dump of information from 10 credit cards that he said were stolen. Based on information from representatives of American Express and

Mastercard, the FBI has confirmed that, of these 10, six American Express credit card numbers and one Mastercard credit card number corresponded to genuine, active accounts belonging to someone other than JARAND MOEN ROMTVEIT, a/k/a "zer0," a/k/a "zer0iq," the defendant.

c. In a chat on or about March 1, 2012, ROMTVEIT provided an address in Norway (the "Norway Address") as the address to which I was to mail the package containing the Apple Laptop (the "Laptop Package"). Later in that same chat, he agreed to pay the shipping cost, of approximately \$200, via Western Union, for the mailing of the Laptop Package from New York to Norway. I asked him to send the shipping payment to my attention (using an undercover alias) in New York, New York. I received the payment of \$200 via Western Union in Manhattan on or about March 7, 2012.

15. In a chat on or about March 2, 2012, JARAND MOEN ROMTVEIT, a/k/a "zer0," a/k/a "zer0iq," the defendant, using the nickname "zer0," said to me: "I got 100% fresh skimmed NJ cards from a hotel . . . I lost the hotel but i managed to pull 72 cards." Based on my training and experience, I know that "credit card skimming" refers to the theft of credit card information used in an otherwise legitimate transaction, often through transactions at restaurants and hotels. I believe that in this chat, ROMTVEIT was explaining that he had managed to obtain information for 72 credit cards recently stolen ("skimmed") from a New Jersey hotel before the hotel realized the theft. Later in that same chat, he said, "i wanna talk to you about doing some more stuff if you want maybe you can sell and send a % ? in cash?" I agreed. The defendant then asked, "when would you like to start and what kinda deal would you be willing to do ?" I responded, "maybe like 70/30, im taking a lot of risk." ROMTVEIT said that he could agree to such an arrangement and noted again that he had "70 100% fresh and valid NJ cards." Based on my experience in this investigation, I believe that ROMTVEIT was proposing a new arrangement whereby he would provide me with the stolen credit card information which I would sell and give him a percentage in cash of what I made from the purported sale. We agreed that he would get 30% of my sale proceeds, and he then reiterated that he had stolen account data from 70 still valid New Jersey-based credit cards. The defendant then provided me with credit card information for approximately 30 cards, as described in greater detail in ¶17.

16. In a chat on or about March 8, 2012, JARAND MOEN

ROMTVEIT, a/k/a "zer0," a/k/a "zer0iq," the defendant, using the nickname "zer0," said "anyway im ready for more when you are," indicating that he was ready to provide more stolen credit card information to me. He later asked, "how many do you want and what type of cards." In response to my question about how many Visa and Mastercards he had information about, he responded "hard to say its like a huge list about 14 000 cards. . . . a lot are out of date so i guess 4-500~ left." Based on my involvement in this investigation, I believe that in this chat the defendant was explaining that while he had a stolen database of approximately 14,000 cards, the ones that were valid and active amounted to approximately 400 to 500 due to the age of the list. Later in that chat, the defendant said he had "checked 30 cards im gonna past them here now." He then proceeded to paste the information from a dump of 30 cards, "all live . . . please try to use them asap." Based on my training and experience, I believe that ROMTVEIT was explaining that the cards about which he was providing information were newly stolen and confirmed to be valid, but the information he provided needed to be used quickly in order to ensure the card information could be exploited before the cards were cancelled due to their use in fraudulent transactions. On or about March 29, 2012, I sent to Norway, via Western Union, addressed to a name provided by the defendant, approximately \$1,100, purportedly his share of the sale proceeds in connection with the exchange we had agreed to as described in ¶16. The credit cards were not, however, actually resold by the FBI. The FBI notified the relevant credit card companies regarding the credit card information that the defendant had provided in order that appropriate victim notifications could be made. Based on information from representatives of American Express, Visa, and Discover, the FBI has confirmed that, of these 30 cards, 26 corresponded to genuine, active accounts belonging to individuals other than JARAND MOEN ROMTVEIT, a/k/a "zer0," a/k/a "zer0iq," the defendant.

17. In a chat on or about March 15, 2012, I asked JARAND MOEN ROMTVEIT, a/k/a "zer0," a/k/a "zer0iq," the defendant, using the nickname "zer0," how many more cards he had. He responded with a breakdown of the number of active cards and corresponding locations: "maybe 40-50 NY thats live 60 x UK 201 6x North Carolina 6x Tennessee 50x New Jersey 9x Minnesota thats about it for now." He later said, "im doing massive bruting all day and i managed to hack 7 cash registers + coffee shop but all dump info was encrypted and it was like 25k dumps lol [laugh out loud] kinda disappointed but yeah this shit takes time, i will get more, its just a question on when :)." Based on my training

and experience, I know that in online hacking terminology "bruting" refers to "brute force password cracking," a method to decode, or "crack," encrypted passwords. In this chat, ROMTVEIT explained that he had spent the day trying to crack passwords through this method and had managed to hack into various entities but the credit card information was encrypted so he could not access it.

Identification of the Defendant

18. As noted above in ¶13d, in a chat on or about February 9, 2012, the defendant, using the nickname "zer0," provided me with a link to what he said was his Facebook account, www.facebook.com/jarandmr. I accessed that account, which was public, and learned that it belonged to an individual named "Jarand Moen" living in Porsgrunn, Norway.

19. As noted above in ¶13d, on or about February 9, 2012, the defendant, using the nickname "zer0," demonstrated to me how to use a particular hacking tool. In the course of the demonstration, I was able to see the name "Jarand Moen" on his computer, which the defendant later confirmed was his real name.

20. As noted above in ¶14, in a series of private chats between on or about February 24, 2012 and March 1, 2012, the defendant, using the nickname "zer0," and I made arrangements for a transaction in which I would send him an Apple Laptop and he would pay for the shipping costs via Western Union. In a chat on or about March 1, 2012, the defendant requested that I address the Laptop Package to "Jarand Moen" at an address in Porsgrunn, Norway (the "Norway Address"). The Western Union payment for the shipping costs, which I received on or about March 7, 2012 in New York, New York, was sent from "Jarand Moen Romtveit" in Norway. In addition, I and other FBI agents confirmed with law enforcement authorities in Norway that, according to public records in Norway, an individual named "Jarand Moen Romtveit" resides at the Norway Address. Based on conversations with law enforcement authorities in Norway, I also learned that the following happened, in sum and substance:

a. The Laptop Package was delivered to the Norway Address on or about March 9, 2012, and "Jarand Moen Romtveit" provided a signature for receipt of the Laptop Package;

b. Norwegian law enforcement officials obtained a photograph from public records of JARAND MOEN ROMTVEIT, the defendant; and


c. Norwegian law enforcement officials showed the courier who made the delivery (the "Courier") a photograph of ROMTVEIT. The Courier confirmed that the individual depicted in the photograph was the individual who had received and signed for the Laptop Package.

21. Accordingly, I believe that the individual using the nickname "zer0," who sold me data for at least 15 stolen credit cards in exchange for at least \$1,100 and a laptop computer as described above, is JARAND MOEN ROMTVEIT, a/k/a "zer0," a/k/a "zer0iq," the defendant.

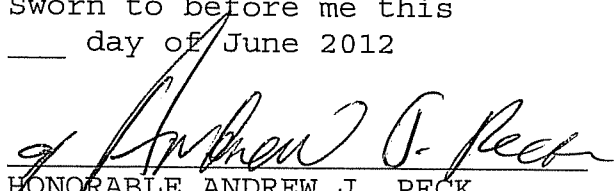
22. From speaking with representatives of American Express, Visa, Discover, and MasterCard, I have confirmed that, in total, at least 36 credit card numbers "zer0" passed to me corresponded to genuine, active accounts belonging to individuals other than JARAND MOEN ROMTVEIT, a/k/a "zer0," a/k/a "zer0iq," the defendant.

WHEREFORE, I respectfully request that an arrest warrant be issued for JARAND MOEN ROMTVEIT, a/k/a "zer0," a/k/a "zer0iq," the defendant, and that he be arrested and imprisoned or bailed, as the case may be.

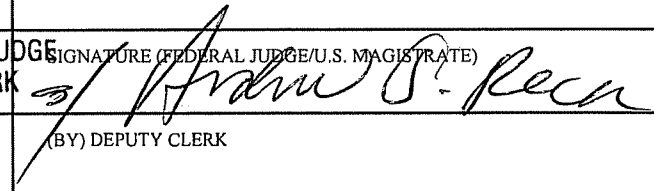
JUN 20 2012


JOHN LEO, JR.
Special Agent
Federal Bureau of Investigation

Sworn to before me this
___ day of June 2012


HONORABLE ANDREW J. PECK
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK

WARRANT FOR ARREST

United States District Court		DISTRICT SOUTHERN DISTRICT OF NEW YORK	
UNITED STATES OF AMERICA v. JARAND MOEN ROMTVEIT, a/k/a "zer0," a/k/a "zer0iq"		DOCKET NO. 12 MAG	MAGISTRATE'S CASE NO. 1656
WARRANT ISSUED ON THE BASIS OF: <input type="checkbox"/> Order of Court <input type="checkbox"/> Indictment <input type="checkbox"/> Information <input checked="" type="checkbox"/> Complaint		NAME AND ADDRESS OF INDIVIDUAL TO BE ARRESTED JARAND MOEN ROMTVEIT, a/k/a "zer0," a/k/a "zer0iq"	
		DISTRICT OF ARREST Southern District of New York	
TO: UNITED STATES MARSHAL OR ANY OTHER AUTHORIZED OFFICER		CITY	
YOU ARE HEREBY COMMANDED to arrest the above-named person and bring that person before the United States District Court to answer to the charge(s) listed below.			
DESCRIPTION OF CHARGES			
Access Device Fraud and Aggravated Identity Theft			
IN VIOLATION OF	UNITED STATES CODE TITLE 18	SECTION § 1029 (a) (3), 1029 (a) (5), 1028A	
BAIL ANDREW J. PECK	OTHER CONDITIONS OF RELEASE		
ORDERED BY UNITED STATES MAGISTRATE JUDGE SOUTHERN DISTRICT OF NEW YORK	SIGNATURE (FEDERAL JUDGE/U.S. MAGISTRATE) 		DATE ORDERED JUN 20 2012
CLERK OF COURT	(BY) DEPUTY CLERK		DATE ISSUED
RETURN			
This warrant was received and executed with the arrest of the above-named person.			
DATE RECEIVED	NAME AND TITLE OF ARRESTING OFFICER	SIGNATURE OF ARRESTING OFFICER	
DATE EXECUTED			

Note: The arresting officer is directed to serve the attached copy of the charge on the defendant at the time this warrant is executed.